 <p>(Enriching the Research)</p>	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

CAPTCHA AS GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Mr . K. Naresh Babu¹, J. Chandini², B. Sowmya³, A. Vinay⁴, A. Sivadevi⁵

¹ Assistant Professor, Department of CSE, Ramachandra College of Engineering, Eluru, A.P

^{2,3,4,5} UG Students, Department of CSE, Ramachandra College of Engineering, Eluru, A.P

ABSTRACT

There is a serious issue of security breaking whether we think about internet services or desktop applications. Old password methods have some downsides, including the potential for password stealing, shoulder-surfing attacks, internet password guessing attacks, and relay attacks. Therefore, there needs to be a system that offers an effective defense against password-cracking attacks. There are numerous methods for it as well as numerous password schemes that can be used to accomplish this. The program's fundamental flaw is that users must go through difficult and time- consuming steps to register and log in because its logic uses powerful AI processes. The typical system user finds these complex AI procedures to be taxing. This project suggest authentication methods such as Captcha technology, which we call Captcha as graphical passwords (CaRP). that include graphical Captchas based on passwords. It comprises of a graphical password system and a Captcha. Although CaRP is not a panacea, it does offer acceptable security and usability and seems to work well with certain useful applications for enhancing online security. When a user logs in, our system offers them a variety of authentication options. It expand the use of a Captcha to include both human identification and a graphical password as a result, it offers all the advantages of a Captcha and strengthens the system from a security viewpoint.


1. INTRODUCTION

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security or the phrase computer security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism.

Diagram clearly explain the about the secure computing

Physical security:

- ☐ Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.
- ☐ Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provide

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

□ The only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

Access passwords:

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

Prying eye protection:

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

Anti-virus software:

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

Firewalls:

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

Software updates:

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.

Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.


Keep secure backups:

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

Report problems:

If you believe that your computer or any data on it has been compromised, you should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

Benefits of secure computing:

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

- ☐ Protect your investment - Free storage
 - ☐ Protect your business – Blackmail
- Protect your income - Competitive advantages.

2. LITERATURE SURVEY

1. On predictive models and user drawn graphical passwords

AUTHORS: P. C. van Oorschot and J. Thorpe

In commonplace text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable to brute-force dictionary attacks. This leads us to ask whether other types of passwords (e.g., graphical) are also vulnerable to dictionary attack because of users tending to choose memorable passwords. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall. These cognitive studies motivate us to define a set of *password complexity factors* (e.g., reflective symmetry and stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak the password subspaces they define might be, we use the “Draw-A-Secret” (DAS) graphical password scheme of Jermyn et al. [1999] as an example. We analyze the size of these classes for DAS under convenient parameter choices and show that they can be combined to define apparently popular subspaces that have bit sizes ranging from 31 to 41—a surprisingly small proportion of the full password space (58 bits). Our results quantitatively support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guidelines and proactive password checking.


2. Modeling user choice in the PassPoints graphical password scheme

AUTHORS: A. E. Dirik, N. Memon, and J.-C. Birget

We develop a model to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our model predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to evaluate automatically whether a given image is well suited for the PassPoints system, and to analyze possible dictionary attacks against the system. We compare the predictions provided by our model to results of experiments involving human users. At this stage, our model and the experiments are small and limited; but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research.

3. Securing passwords against dictionary attacks

AUTHORS: B. Pinkas and T. Sander

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user's perspective user-friendliness is a key requirement. In this paper we suggest a novel authentication scheme that preserves the advantages of conventional password authentication, while simultaneously raising the costs of online dictionary attacks by orders of magnitude. The proposed scheme is easy to implement and overcomes some of the difficulties of previously suggested methods of improving the security of user authentication schemes. Our key idea is to efficiently combine traditional password authentication with a challenge that is very easy to answer by human users, but is (almost) infeasible for automated programs attempting to run dictionary attacks. This is done without affecting the usability of the system. The proposed scheme also provides better protection against denial of service attacks against user accounts.

4. Revisiting defenses against large-scale online password guessing attacks


AUTHORS: M. Alsaleh, M. Mannan, and P. C. van Oorschot

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. In this paper, we discuss the inadequacy of existing and proposed login protocols designed to address large-scale online dictionary attacks (e.g., from a botnet of hundreds of thousands of nodes). We propose a new Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT. We analyze the performance of PGRP with two real-world data sets and find it more promising than existing proposals.

5. Cognitive authentication schemes safe against spyware

AUTHORS: D. Weinshall

Can we secure user authentication against eavesdropping adversaries, relying on human cognitive functions alone, unassisted by any external computational device? To accomplish this goal, we propose challenge response protocols that rely on a shared secret set of pictures. Under the brute-force attack the protocols are safe against eavesdropping, in that an observer who fully records any feasible series of successful interactions cannot practically compute the user's secret. Moreover, the protocols can be tuned to any desired level of security against random guessing, where security can be traded-off with authentication time. The proposed

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

protocols have two drawbacks: First, training is required to familiarize the user with the secret set of pictures. Second, depending on the level of security required, entry time can be significantly longer than with alternative methods. We describe user studies showing that people can use these protocols successfully, and quantify the time it takes for training and for successful authentication. We show evidence that the secret can be effortlessly maintained for a long time (up to a year) with relatively low loss.

3. EXISTING SYSTEM

- Attribute-based encryption schemes have been The most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots.
- To use Captcha in authentication there was system that uses Captcha and password in a user authentication protocol, which was called Captcha-based Password Authentication (CbPA) Protocol.
- The CbPA – protocol requires solving a Captcha challenge after inputting a valid pair of user id and password.
- The server sends a challenge text is the same as the sent challenge text and the client is authenticated.

LIMITATIONS:


- This existing paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Another one is Shoulder Surfing attack which means it is looking over someones shoulder when they enter a password or a PIN code.

4. PROPOSED SYSTEM

- In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP).
- CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks.
- CaRPs can be implemented on both text and image recognition Captcha.

ADVANTAGES:

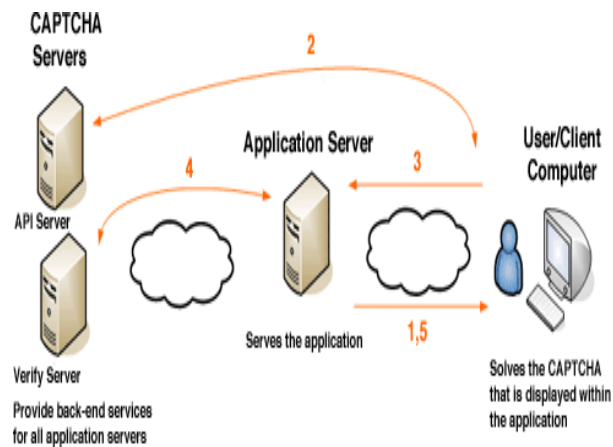
- CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.
- CaRP also offers protection against relay attacks, an increasing threat to bypass Captcha protection.

 (Enriching the Research)	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

- CaRP can protect from spammers, which increases the spammer's operational costs and also reduces spam emails.
- CaRP also can prevent shoulder surfing attacks if it is combined with dual-view technologies.
- CaRP helps to protect against spam bots from entering an email account even if they know the password.

CaRP can be applied on touch-screen devices where typing passwords are difficult especially for e-banks to secure internet applications.

System Architecture



5. RESULTS

HOME PAGE


 <p>IJESAT (Enriching the Research)</p>	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023



Fig2: Displaying home page

USER REGISTRATION

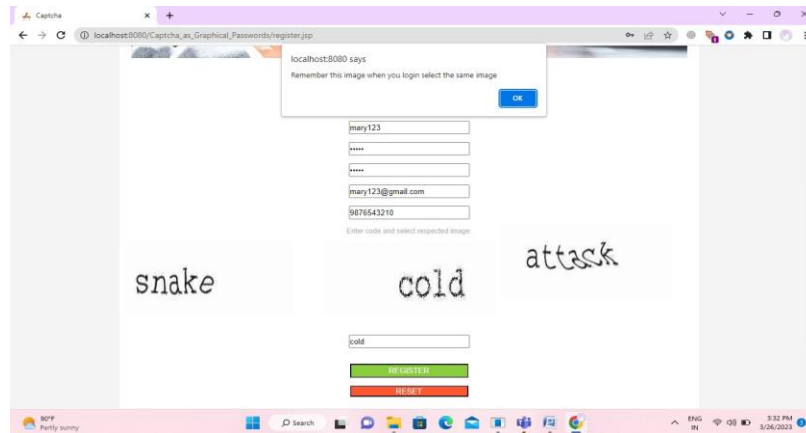


Fig3: Shows the user registration page

USER LOGIN (Userid with password and captcha)

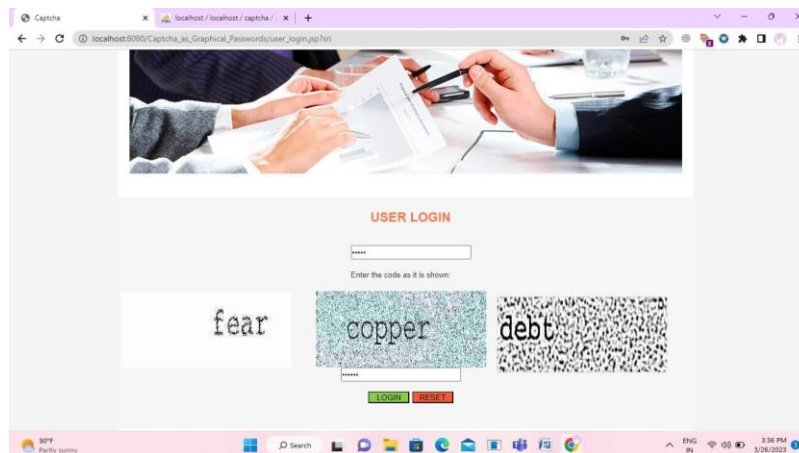


Fig4: User login with userid with password & Captcha

SUCCESSFULLY LOGIN

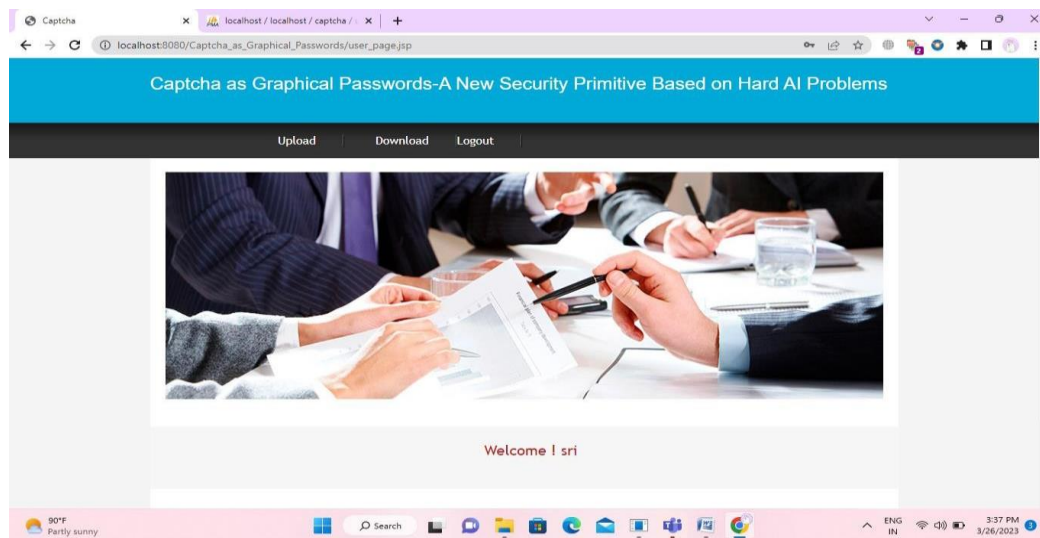


Fig5: User login successfully

FILE UPLOADING(using valid coordinates)

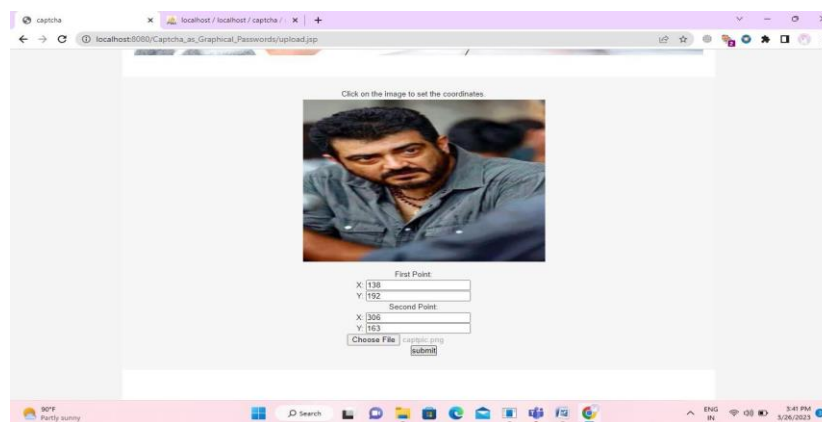
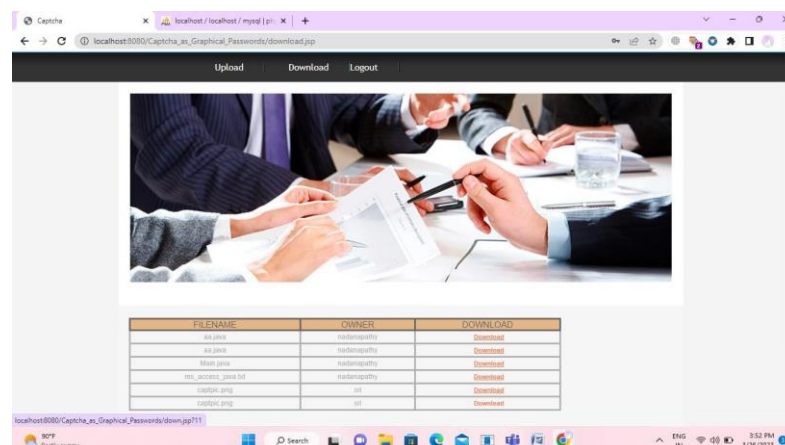


Fig6: User can upload the required file

DOWNLOAD FILE



 <p>IJESAT (Enriching the Research)</p>	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

Fig7: User can download the uploaded file

INVALID COORDINATES

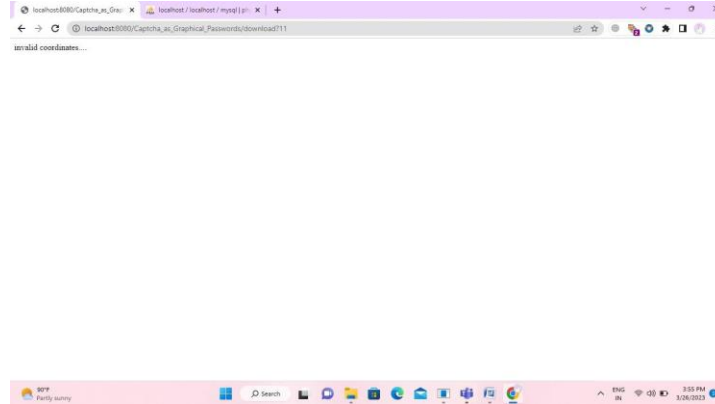


Fig8: It gives the alert when user enter invalid coordinates

ADMIN LOGIN

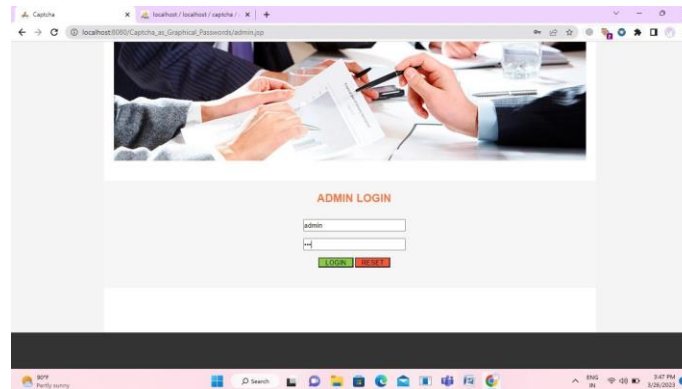
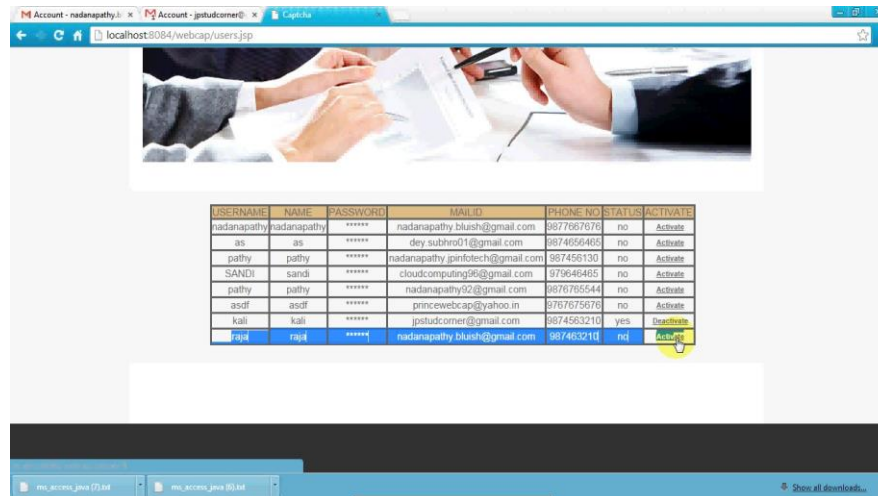


Fig9: Admin login to their account

ADMIN ACTIVATING USER




 (Enriching the Research)	Open Access Research Article		
	Volume: 23 Issue: 07		
	July, 2023		

Fig10: Admin activating the user**ADMIN ACTIIVATING BLOCKED USER****Fig11: Admin activating the blocked user****6. CONCLUSION**

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service.

Our usability study of two CaRP schemes we have implemented is encouraging. For example, more participants considered AnimalGrid and ClickText easier to use than PassPoints and a combination of text password and Captcha. Both AnimalGrid and ClickText had better password memorability than the conventional text passwords. On the other hand, the usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in. The optimal tradeoff between security and usability remains an open question for CaRP, and further studies are needed to refine CaRP for actual deployments.

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

Like Captcha, CaRP utilizes unsolved AI problems. However, a password is much more valuable to attackers than a free email account that Captcha is typically used to protect. Therefore there are more incentives for attackers to hack CaRP than Captcha. That is, more efforts will be attracted to the following win-win game by CaRP than


ordinary Captcha: If attackers succeed, they contribute to improving AI by providing solutions to open problems such as segmenting 2D texts. Otherwise, our system stays secure, contributing to practical security. As a framework, CaRP does not rely on any specific Captcha scheme. When one Captcha scheme is broken, a new and more secure one may appear and be converted to a CaRP scheme. Overall, our work is one step forward in the paradigm of using hard AI problems for security. Of reasonable security and usability and practical applications, CaRP has good potential for refinements, which call for useful future work. More importantly, we expect CaRP to inspire new inventions of such AI based security primitives.

FUTURE ENHANCEMENT

Due to use of multiple schemes into one system, password space is increased to great extent. We can apply Captcha as Graphical Password authentication schemes where we have to provide security to extra sensitive data. In future, work on the implementation of CaRP schemes in virtual environment and improvement work in usability can be done.

REFERENCES

- [1] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” *ACM Comput. Surveys*, vol. 44, no. 4, 2012.
- [2] H. Tao and C. Adams, “Pass-Go: A proposal to improve the usability of graphical passwords,” *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008.
- [3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005.
- [4] P. C. van Oorschot and J. Thorpe, “On predictive models and userdrawn graphical passwords,” *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.
- [5] K. Golofit, “Click passwords under investigation,” in *Proc. ESORICS*, 2007, pp. 343–358.
- [6] A. E. Dirik, N. Memon, and J.-C. Birget, “Modeling user choice in the passpoints graphical password scheme,” in *Proc. Symp. Usable Privacy Security*, 2007, pp. 20–28.
- [7] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in clickbased graphical passwords,” *J. Comput. Security*, vol. 19, no. 4, pp. 669–702, 2011.
- [8] P. C. van Oorschot and S. Stubblebine, “On countering online dictionary attacks with login histories and humans-in-the-loop,” *ACM Trans. Inf. Syst. Security*, vol. 9, no. 3, pp. 235–258, 2006.
- [9] M. Alsaleh, M. Mannan, and P. C. van Oorschot, “Revisiting defenses against large-scale online password guessing attacks,” *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.
- [10] S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using cued click points,” in *Proc. ESORICS*, 2007, pp. 359–374.

	Open Access Research Article
	Volume: 23 Issue: 07
	July, 2023

- [11] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, “Influencing users towards better passwords: Persuasive cued click-points,” in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1. 2008, pp. 121–130.
- [12] P. Golle, “Machine learning attacks against the Asirra CAPTCHA,” in Proc. ACM CCS, 2008, pp. 535–542.
- [13] B. B. Zhu et al., “Attacks and design of image recognition CAPTCHAs,” in Proc. ACM CCS, 2010, pp. 187–200.
- [14] J. Yan and A. S. El Ahmad, “A low-cost attack on a Microsoft CAPTCHA,” in Proc. ACM CCS, 2008, pp. 543–554.
- [15] J. Elson, J. R. Douceur, J. Howell, and J. Saul, “Asirra: A CAPTCHA that exploits interest-aligned manual image categorization,” in Proc. ACM CCS, 2007, pp. 366–374.
- [16] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, “A new CAPTCHA interface design for mobile devices,” in Proc. 12th Austral. User Inter. Conf., 2011, pp. 3–8.
- [17] N. Joshi. (2009, Nov. 29). Koobface Worm Asks for CAPTCHA [Online]. Available: <http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor-CAPTCHA>
- [18] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, “Re: CAPTCHAs—Understanding CAPTCHA-Solving Services in an Economic Context,” in Proc. USENIX Security, 2010, pp. 435–452.
- [19] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, “Breaking e-banking CAPTCHAs,” in Proc. ACSAC, 2010, pp. 1–10.
- [20] H. Gao, X. Liu, S. Wang, and R. Dai, “A new graphical password scheme against spyware by using CAPTCHA,” in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.